401. Second, the appendix does not contain any source code showing the integration between P-BEST and the rest of eXpert. The appendix contains version 2.2 of the source code file eXpert.c.[183] This version of eXpert.c contains none of the code related to the integration between the rest of eXpert and P-BEST. Prior to the summer of 1998, the code that integrated P-BEST with the rest of eXpert was contained in the source code file eXpert.c. However, in the summer of 1998, SRI moved this integration code and much of the functionality of eXpert.c into a source code file called event.c.[184] Versions 2.0 and later of eXpert.c do not contain this integration code. SRI included version 2.2 of eXpert.c in the appendix, but failed to include event.c. The result is that SRI failed to include in the appendix any file that showed how P-BEST was integrated with the rest of eXpert.

402. Third, the appendix contains none of the files—listed in Exhibit AA—containing P-BEST signatures. In fact, the nine hundred plus page source code appendix does not contain a single P-BEST rule.

403. I also analyzed the patents-in-suit and the two articles incorporated by reference[185] into the patents-in-suit to determine whether any of those documents contained information related to P-BEST, the integration of P-BEST with the rest of eXpert, or the suite of P-BEST rules that SRI wrote to detect suspicious network activity. I found no discussion of P-BEST, the integration of P-BEST with the rest of eXpert, or the suite of rules that SRI wrote to analyze network traffic data and detect suspicious activity in any of those documents.

---

[183] *See* [SYM_P_0549715-18].
[184] *See* SRI Source Code REQUESTS #19, #20, #23.
[185] As explained previously in my report, it is my understanding that SRI has admitted that these two articles may not be used for satisfying the best mode requirement. Nevertheless, in an abundance of caution, I analyzed them anyway.

404. To summarize, it is my opinion that the signature engine eXpert was SRI's best mode as of November 9, 1998 for detecting suspicious network activity. It is also my opinion that SRI failed to sufficiently disclose eXpert.

D. etcpgen, SRI's best mode for performing network monitoring, was not disclosed

405. Another SRI software component that I analyzed was etcpgen. etcpgen was a software component that processed raw packets into the EMERALD message format. Mr. Porras has testified that, as of the filing date of the patent, etcpgen was SRI's best mode for performing "network surveillance" or "network monitoring" as required by the claims.[186] etcpgen had a number of useful features. For example, it could analyze a number of different network packet formats, including TCP, IP, UDP, ICMP, and ARP. Based on my review of the source code that SRI placed into escrow, it is my opinion that etcpgen was the inventors' best mode for performing network monitoring. The files listed in Exhibit DD were part of the code base for etcpgen as of November 9, 1998.

406. Having determined that etcpgen was the inventors' best mode for performing network monitoring, I then analyzed the appendix to the patents-in-suit to determine whether code for etcpgen was contained in the appendix to the patents in suit. I found none of the source code files for etcpgen—listed in Exhibit DD—in the appendix to the patents-in-suit.

407. I also analyzed the shared written description of the patents-in-suit and the articles incorporated by reference into the written description. I found no mention of etcpgen.

[186] Porras 30(b)(6) Tr. 173:10-174:24.

408. To summarize, it is my opinion that etcpgen was the inventors' best mode for performing network monitoring. I have also determined that etcpgen was not disclosed. Therefore, by failing to disclose etcpgen, the inventors failed to disclose their best mode for performing network monitoring.

E. eResolve, SRI's best mode for performing response, was not disclosed

409. Another SRI software component that I analyzed was eResolve. I understand Mr. Porras has testified[187] that either estat or eResolve was SRI's best mode for practicing "responding" or "invoking countermeasures" (generically "response") as claimed in the patents-in-suit. eResolve was a software component that received alerts from both estat and eXpert. eResolve allowed the administrator of the instrusion detection system to set a policy regarding which types of alerts to report to a higher-level entity.

410. I have determined that the files listed in Exhibit EE are part of the code base for eResolve as it existed prior to November 9. 1998. Based on my analysis of these files, I have determined that prior to November 9, 1998 SRI had implemented a complete version of eResolve.

411. None of the files listed in Exhibit EE are contained in the appendix to the patents-in-suit. Furthermore, there is no mention of eResolve in the patents-in-suit or the articles incorporated by reference into the patents-in-suit.

412. To summarize, it is my opinion that eResolve was the inventors' best mode for performing response. I have also determined that eResolve was not disclosed. Therefore, by failing to disclose eResolve, the inventors failed to disclose their best mode for performing response.

---

[187] Porras 30(b)(6) Tr. 180:7-183:7.

XIII. ENABLEMENT AND SUFFICIENT WRITTEN DESCRIPTION OF THE PATENTS-IN-SUIT

A. Legal standard

413. I understand that the specification of a patent must provide an enabling disclosure. I understand that this requires that a person of skill in the art, using knowledge available to them and the disclosure in the patent, could make and use the invention without undue experimentation. I also understand that the enablement standard for prior art publications is similar to that required for a patent specification.

414. I have been informed that the factors to be assessed in determining whether experimentation is "undue" include: the quantity of experimentation necessary, the amount of direction or guidance presented, the presence or absence of working examples, the nature of the invention, the state of the prior art, the relative skill of those in the art, the predictability or unpredictability of the art, and the breadth of the claims.

415. I also understand that the specification of a patent must describe the subject matter claimed in the patent in a manner that conveys to one of skill in the art that the inventors had possession of the subject matter claimed at the time the patent application was filed.

B. Analysis of enablement / written description

416. I understand that SRI contends that the disclosures in certain prior art references, including *Emerald 1997*, are not enabling for certain claim limitations.[188] It is my opinion that the prior art references discussed in my report, including *Emerald 1997*, are enabling and provide a disclosure at the same general level of detail as found in the

[188] For example, SRI has claimed that Emerald 1997 does not provide an enabling disclosure of a statistical detection method. *See* SRI International, Inc,'s "Amended" Response to Symantec's Invalidity and Inequitable Conduct Contentions (Dec. 16, 2005).

specification of the patents-in-suit. In particular, given the overall similarity between the disclosures in *Emerald 1997* and the patents-in-suit, including substantial portions of identical text and identical figures, it is not plausible to claim that one is enabled, but the other is not.

417. In particular, with regard to the disclosure in the patents-in-suit regarding statistical profiling / statistical detection method, I believe the written description of the patents alone sufficiently enables statistical profiling. As noted previously in my report, SRI has stated that the *Statistical Methods* paper is not "essential material" as defined by the USPTO, which means the paper is not required in order for the patents to be enabled. In my opinion, the algorithms disclosed in *Statistical Methods* would not be required for one of skill in the art to use the disclosures in the patents-in-suit to perform statistical profiling generally.[189]

418. In addition, I do not believe that the code included in the appendix to the patents-in-suit is required in order for the patents to be enabled. One of the inventors, Mr. Valdes, agreed.[190] The 1000+ pages of code in the appendix do include large portions of SRI's estat code base, which was used to implement statistical profiling. However, this code provides minimal commentary, and thus is extremely difficult to understand. I do not believe it would have been practical for someone with no familiarity with the code to reverse-engineer the statistical profiling algorithms from the appendix.[191] It would have been simpler for one of skill to use the patent specification's description of

---

[189] However, even if SRI contents the algorithms in *Statistical Methods* are required for enablement, this paper was publicly available as of 1995 and thus these algorithms were already known in the field. These algorithms would have been obvious to combine with a system such as that disclosed in *Emerald 1997*.

[190] Valdes Tr. 561.

[191] Valdes Tr. 558-559 (stating that it would be "much harder" to reverse engineer the statistical profiling algorithms from the source code than the NIDES algorithms).

statistical profiling combined with his or her existing knowledge of intrusion detection to implement a statistical profiling method.

419. To the extent that SRI claims that particular pieces of prior art, including *Emerald 1997*, are not enabling, my opinion is that this would necessitate a finding that the patents-in-suit themselves similarly do not satisfy the enablement and written description requirements.

420. I understand that certain SRI personnel, including the inventors of the patents-in-suit, have continued to file additional patent applications after the filing of the '338 application that led to the patents-in-suit. It is my opinion that the alleged inventions disclosed in these later-filed applications are not described in the patents-in-suit.

421. For example, after filing the application that matured into the '338 patent, the inventors filed applications relating to the use of Baysian algorithms in intrusion detection.[192] As the inventors have admitted, Baysian algorithms are not disclosed in the patents-in-suit and therefore are not part of the alleged inventions claimed in the patents-in-suit.[193] Similarly, the inventors also filed patent applications on later work done on alert correlation methods such as probabilistic alert correlation.[194] As discussed previously in my report, the patents-in-suit provide a very minimal description of correlation. Later work done by SRI on correlation methods such as probabilistic alert

---

[192] *See, e.g.*, A. Valdes, K. Skinner and P. Porras, Application No. 09/653,066 "Methods for Detecting and Diagnosing Abnormalities Using Real-Time Bayes Networks," filed 9/1/2000; A. Valdes, M. Fong and P. Porras, Application No. 09/952,080 "Prioritizing Bayes Network Alerts," filed 9/13/2001.
[193] Porras 30(b)(6) Tr. 250-251; Valdes Tr. 231-232, 315-316.
[194] *See, e.g.*, A. Valdes and K. Skinner, Application No. 09/944,788 "Probabilistic Alert Correlation," filed 8/31/2001.

correlation is not disclosed in the patents-in-suit and therefore is not part of the alleged inventions claimed in the patents-in-suit.[195]

XIV. PUBLIC AVAILABILITY OF CERTAIN DOCUMENTS

422. I am a named author on the paper: Steven Snapp et al., "Intrusion Detection Systems (IDS): A Survey of Existing Systems and A Proposed Distributed IDS Architecture" CSE-91-7 (February 1991) ("DIDS February 1991") [SYM_P_0069280-SYM_P_0069297]. This paper was publicly available as of 1991. The "CSE-91-7" indicates that this paper was a technical report, filed with the UC Davis Division of Computer Science. Such technical reports could be requested from the Division and were publicly available. In fact, this paper has been cited by other authors not associated with UC Davis, see, e.g., G. White et al., "Cooperating Security Managers: A Peer-Based Intrusion Detection System," IEEE Network, Jan./Feb. 1996 at [9].

423. I am a named author on the paper: B. Mukherjee et al., "Network Intrusion Detection" IEEE Network, Vol. 8 No. 3, pp. 26-41, May/June 1994 [SYM_P_0069263-SYM_P_0069279] see also [SRI 058251-058266]. As indicated by the IEEE Network magazine cover page, this article was published and publicly available as of the indicated date.

424. I have spoken to Mr. Staniford, a named author on the paper: Staniford-Chen, S., et al. "GrIDS - A graph based intrusion detection system for large networks," 19th National Information Systems Security Conference, 1996 ("GrIDS 1996") [SYM_P_0068883-SYM_P_0068892]. Based upon our discussion, I understand that this paper was published and publicly available in the 19th NISSC conference proceedings, which were distributed to all conference attendees.

---

[195] Valdes Tr. 234.

425. I have spoken to Mr. Staniford, a named author on the paper: Steven Cheung, Rick Crawford, Mark Dilger, Jeremy Frank, Jim Hoagland, Karl Levitt, Stuart Staniford-Chen, Raymond Yip, Dan Zerkle, "The Design of GRIDS: A Graph-Based Intrusion Detection System," Technical report, UC Davis Department of Computer Science, Davis California (May 14, 1997) (GrIDS 1997") [SYM_P_0080878-SYM_P_0080943]. Based upon our discussion, I understand that Mr. Staniford posted this paper to the GrIDS home page by 1996. The document was regularly updated through 1997. Furthermore, the Internet Archive demonstrates this paper was publicly available at least as early as July 19, 1997. *See* SYM_P_0512090 - SYM_P_0512181.

426. I have spoken to Mr. Smaha, the author of the Stalker line of products. Based upon our conversation, I understand that NetStalker, Installation and User's Guide, Version 1.0.2 1996 [SYM_P_0079550- SYM_P_0079629] was distributed to customers with versions of the NetStalker product prior to Nov. 1997. I also understand that employees of Tivoli actually tested the NetStalker product with Tivoli, a network management application.

427. Based upon my review of the University of New Mexico's on-line catalog, I believe the publication: Richard Heady, George Luger, Arthur Maccabe, and Mark Servilla, "The Architecture of a Network Level Intrusion Detection System," Technical Report CS90-20, University of New Mexico, Department of Computer Science, August 1990 [SYM_P_050086- SYM_P_0500603] was cataloged at UNM and publicly available prior to Nov. 9, 1997. *See* [SYM_P_0535342].

428. As indicated in the Hansen and Berard declarations in Exhibit HH, the thesis: Feather, Frank Edward, Ph.D., "Fault Detection in an Ethernet network via anomaly detectors," Carnegie Mellon University, Order number 9224199 (1992) [SYM_P_0501779- SYM_P_0502036] was cataloged and publicly available prior to Nov. 9, 1997.

432. I have spoken to Mr. Staniford, the moderator for the CIDF mailing list. Based upon my conversation with him, as well as my own personal recollection and my review of Internet Archive documentation relating to CIDF, it is my opinion that documentation and emails distributed to the CIDF mailing list were archived publicly on the CIDF website contemporaneously with their distribution. *See, e.g.*, Mr. Stanford's email setting up this archive [SYM_P_0603086].

Dated: April 21, 2006

Louis Todd Heberlein

L. Todd Heberlein

L

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation,

Plaintiff,

vs.

INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation,

Defendants.
_____/

COPY

Case No. 04-1199-SLR

Deposition of

L. TODD HEBERLEIN

June 2, 2006

Volume I
Pp. 1-238

Reported by
John Wissenbach, CSR 6862

SHARI MOSS & ASSOCIATES
Certified Shorthand Reporters
110 Sutter Street, Suite 607
San Francisco, California 94104
(415) 402-0004
(650) 692-8900
FAX: (415) 402-0005

16:30:18 Going off the record, the time is 4:30 p.m.
16:39:23 (Recess taken.)
16:39:38 THE VIDEOGRAPHER: Back on the record.
16:39:46 Here marks the beginning of tape number 4 in the
16:39:50 deposition of Todd Heberlein. The time is 4:39 p.m.
16:39:55 BY MR. POLLACK:
16:39:55 Q. Mr. Heberlein, I'd like to refer you to
16:39:57 page 85 of your report, Exhibit 619, paragraph 261.
16:40:09 And in that paragraph, you refer to two documents:
16:40:13 one you refer to as "Live Traffic Analysis"; and the
16:40:17 other, "EMERALD, Conceptual Design 1997." Do you
16:40:22 see that?
16:40:22 A. Uh-huh. Yes.
16:40:22 Q. Am I correct in understanding that you're
16:40:24 not offering any opinions as to whether or not,
16:40:27 starting with Live Traffic Analysis, that that --
16:40:29 whether or not that paper is in fact prior art,
16:40:32 correct?
16:40:35 MS. BROWN: Objection; misstates the
16:40:38 testimony -- misstates the document.
16:40:39 THE WITNESS: We believed it would
16:40:42 invalidate many of the claims, although we did not
16:40:45 develop a claim chart.
16:40:48 BY MR. POLLACK:
16:40:48 Q. Actually, what I'm asking you is, you

16:40:51 state, "I understand that there is a debate over
16:40:54 whether or not these documents were publicly
16:40:57 available prior to November 9th, 1997." Do you see
16:41:00 that in your report?
16:41:01 A. Yes, I do.
16:41:02 Q. You're not rendering any opinion in this
16:41:04 case as to whether in fact those documents were
16:41:07 publicly available, correct?
16:41:08 A. Oh. I am not rendering an opinion on that.
16:41:11 Q. Okay. So you're presuming, for the
16:41:14 purposes of your analysis, that they were publicly
16:41:16 available and leaving it up to others to decide that
16:41:20 question, correct?
16:41:32 A. I don't think I'm saying I presume it one
16:41:34 way or the other. I'm just saying if they are, this
16:41:37 is the situation.
16:41:42 Q. Okay. In the next paragraph in your
16:41:45 report, paragraph 262 -- actually, it's 262 through
16:41:53 264. You refer to the EMERALD 1997 paper, which
16:41:59 we've discussed, something called Intrusive Activity
16:42:03 1991, and NIDES 1994.
16:42:06 In paragraph 264, you state, "Given these
16:42:11 explicit references in EMERALD 1997 to both NIDES
16:42:15 1994 and Intrusive Activity 1991, these three
16:42:20 references should be considered to be a single

M
(Redacted in its entirety)

CERTIFICATE OF SERVICE

I hereby certify that on July 24, 2006, I electronically filed the **PUBLIC VERSION** of **SRI INTERNATIONAL, INC.'S OPPOSITION TO ISS' MOTION TO PRECLUDE SRI, BASED ON ITS CONDUCT IN DISCOVERY, FROM DISPUTING THE EVIDENCE ESTABLISHING THAT THE *LIVE TRAFFIC* PAPER IS A 102(b) INVALIDATING REFERENCE** with the Clerk of Court using CM/ECF which will send electronic notification of such filing(s) to the following Delaware counsel. In addition, the document will be served by hand on Delaware counsel as follows:

Richard L. Horwitz Potter Anderson & Corroon LLP Hercules Plaza 1313 North Market Street, 6th Floor P.O. Box 951 Wilmington, DE 19899	Attorneys for Defendant-Counterclaimant Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation
Richard K. Herrmann Morris James Hitchens & Williams PNC Bank Center 222 Delaware Avenue, 10th Floor P.O. Box 2306 Wilmington, DE 19899-2306	Attorneys for Defendant-Counterclaimant Symantec Corporation

I hereby certify that on July 24, 2006, I have sent the foregoing document by Federal Express overnight delivery to the following non-registered participants:

Holmes J. Hawkins, III Natasha Horne Moffitt King & Spalding LLP 1180 Peachtree Street, NE Atlanta, GA 30309	Attorneys for Defendant-Counterclaimant Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation

Paul S. Grewal
Robert M. Galvin.
Lloyd R. Day, Jr.
Day Casebeer Madrid & Batchelder, LLP
20300 Stevens Creek Boulevard, Suite 400
Cupertino, CA 95014

Attorneys for Defendant-Counterclaimant Symantec Corporation

Theresa A. Moehlman
Bhavana Joneja
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036

Defendant-Counterclaimant Internet Security Systems, Inc., a Delaware Corporation, and Internet Security Systems, Inc., a Georgia Corporation

/s/ *John F. Horvath*
John F. Horvath

SRI 724 brief cos.doc